Office of Information Security Newsletter

January 2006
Volume 1 Issue 2

INSIDE THIS ISSUE

Some computer users have an "it's not mine" attitude about the use of their work PC, akin to the difference between how renters feel about their apartments and home owners think of their homes.
(Quote from TechWeb News)

COMPUTER MISUSE NOT HARMLESS FUN

The next song or game you download may put your unit, your job or even the citizens of Nevada at risk.

What might seem like an innocent way to use your break time could allow spyware, aggressive, malicious software or intruders directly into the state system. This activity often requires downloading unauthorized software onto a State computer which to say the least is against state security standard 4.10 section 6b.

This problem is widespread, even in the private sector. Some of the major Internet companies have formed a coalition to put a stop to sites and advertisers that knowingly download spyware, adware, trackware and other malicious software. (For an explanation of some of these terms see the glossary of terms on the OIS website) Some applications are capable of recording every keystroke and sending that information to unknown and often untraceable entities.

The next time you logon to your computer, after you have downloaded the latest game or selected your team for fantasy football, you could be sending confidential information about yourself or the state directly to a terrorist, hacker or some other criminal. That official document saved on your system may contain personal information about yourself or our citizens, such as social security numbers that can be unknowingly shared as a result of the illegal software installation.

This information is sent without any indications or warnings, and once it is sent out it can never be recovered. In addition some 9.9 million individuals were affected by identity theft last year.

The State of Nevada is taking this very seriously because of the potential harm to our state government and its citizens.

Is an online game or a few new songs really worth the risk?

If you would like to learn more about how you can help keep our state safe from cyber threats please take the online security training located at http://infosec.intranet.nv.gov.

BEWARE OF PHISHING

Don't let phishing attempts lure you into the deep end.

What is Phishing? (pronounced "fishing")

A perpetrator sends out legitimate-looking emails appearing to come from some of the Web's biggest sites, including, but not limited to eBay, PayPal, MSN, Yahoo, BestBuy, America Online, Bank of the West and Bank of America, in an effort to phish for personal and financial information from a recipient.

"Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a website that looks just like a legitimate organization's, but isn't. What is the purpose of the bogus site? To trick you into divulging your personal information so the operator can impersonate your identity and run up bills or commit crimes in your name.

Don't take the bait: don't open unsolicited or unknown email messages; don't open attachments from people you don't know or don't expect; and never reply to or click on links in email or pop-ups that ask for personal information. This applies whether on your home PC or on your work desktop or laptop.

KEEP YOUR FAMILY MEMBERS INFORMED:

Elderly Family Members: If you are directed to a website to update your information, verify that the site is legitimate by calling the company directly, using contact information from your account statements. Or open a new browser window and type the known web address into the address field, watching that the actual web address of the site you visit doesn't change and is still the one you intended to visit. To ensure your not being victimized and to detect unauthorized purchases, you should use the same practices you would in the offline world. Check your credit card bill at least every month, and consider using services that inform you if someone has requested credit in your name.

Children Family Members: There are some very important things to remind your children of when their on the computer at home or at school. Remind them to never give out personal information such as their name, home address, school name, or telephone number in a chat room or on bulletin boards. Also, never send their picture to someone they chat with on the computer without your permission.

For more helpful information to keep our children safe visit the links section of the OIS website there's information just for kids.

Defending Nevada's Technology

State of Nevada
Office of Information Security - DoIT
1340 S. Curry Street
Carson City, NV 89703
Phone (775) 684-5800
Fax (775) 687-1155
Email: infosec@state.nv.us
Website: http://infosec.nv.gov